Enhanced Test Command

The Enhanced Test Command feature allows a named user profile to be created with calling line ID (CLID) or dialed number identification service (DNIS) attribute values. The CLID or DNIS attribute values can be associated with the RADIUS record that is sent with the user profile so that the RADIUS server can access CLID or DNIS attribute information for all incoming calls.

- Finding Feature Information, on page 1
- Restrictions for the Enhanced Test Command, on page 1
- How to Configure the Enhanced Test Command, on page 2
- Configuration Examples for Enhanced Test Command, on page 3
- Additional References, on page 4
- Feature Information for Enhanced Test Command, on page 5
- Glossary, on page 5

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for the Enhanced Test Command

The **test aaa group** command does not work with TACACS+.

How to Configure the Enhanced Test Command

Configuring a User Profile and Associating it with the RADIUS Record

This section describes how to create a named user profile with CLID or DNIS attribute values and associate it with the RADIUS record.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa user profile** *profile-name*
4. **aaa attribute** {**dnis** | **clid**}
5. **exit**
6. Router# **test aaa group** {*group-name* | **radius**} *username password* **new-code** [**profile** *profile-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa user profile** *profile-name* **Example:** `Router(config)# aaa user profile profilename1`	Creates a user profile.
Step 4	**aaa attribute** {**dnis**	**clid**} **Example:** `Router# configure terminal`	Adds DNIS or CLID attribute values to the user profile and enters AAA-user configuration mode.
Step 5	**exit**	Exit Global Configuration mode.
Step 6	Router# **test aaa group** {*group-name*	**radius**} *username password* **new-code** [**profile** *profile-name*] **Example:**	Associates a DNIS or CLID named user profile with the record sent to the RADIUS server. **Note** The *profile-name* must match the *profile-name* specified in the **aaa user profile** command.

	Command or Action	Purpose
	`Router# test aaa group radius secret new-code profile profilename1`	

Verifying the Enhanced Test Command Configuration

To verify the Enhanced Test Command configuration, use the following commands in privileged EXEC mode:

Command	Purpose
`Device# debug radius`	Displays information associated with RADIUS.
`Device# more system:running-config`	Displays the contents of the current running configuration file. (Note that the **more system:running-config** command has replaced the **show running-config** command.)

Configuration Examples for Enhanced Test Command

User Profile Associated with a test aaa group command Example

The following example shows how to configure the dnis = dnisvalue user profile “prfl1” and associate it with a **test aaa group** command. In this example, the **debug radius** command has been enabled and the output follows the configuration.

```
aaa user profile prfl1
  aaa attribute dnis
  aaa attribute dnis dnisvalue
  no aaa attribute clid
! Attribute not found.
  aaa attribute clid clidvalue
  no aaa attribute clid
  exit
!
! Associate the dnis user profile with the test aaa group command.
test aaa group radius user1 pass new-code profile profl1
!
!
!
! debug radius output, which shows that the dnis value has been passed to the radius !
server.
*Dec 31 16:35:48: RADIUS: Sending packet for Unique id = 0
 *Dec 31 16:35:48: RADIUS: Initial Transmit unknown id 8 172.22.71.21:1645, Access-Request,
 len 68
 *Dec 31 16:35:48: RADIUS: code=Access-Request id=08 len=0068
         authenticator=1E CA 13 F2 E2 81 57 4C - 02 EA AF 9D 30 D9 97 90
         T=User-Password[2]                L=12 V=*
         T=User-Name[1]                    L=07 V="test"
         T=Called-Station-Id[30]           L=0B V="dnisvalue"
         T=Service-Type[6]                 L=06 V=Login                    [1]
         T=NAS-IP-Address[4]               L=06 V=10.0.1.81
```

```
*Dec 31 16:35:48: RADIUS: Received from id 8 172.22.71.21:1645, Access-Accept, len 38
*Dec 31 16:35:48: RADIUS: code=Access-Accept id=08 len=0038
```

Additional References

The following sections provide references related to Enhanced Test Command.

Related Documents

Related Topic	Document Title
Security Commands	*Cisco IOS Security Command Reference*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Enhanced Test Command

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Enhanced Test Command

Feature Name	Releases	Feature Information
Enhanced Test Command	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.3S	The Enhanced Test Command feature allows a named user profile to be created with calling line ID (CLID) or Dialed Number Identification Service (DNIS) attribute values. The CLID or DNIS attribute values can be associated with the RADIUS record that is sent with the user profile so that the RADIUS server can access CLID or DNIS attribute In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers. The following commands were introduced or modified by this feature: **aaa attribute**, **aaa user profile**, **test aaa group.**

Glossary

AAA --authentication, authorization, and accounting. Suite of network security services that provide the primary framework through which access control can be set up on your Cisco router or access server.

Acct-Session-ID (attribute 44) --A unique accounting identifier that makes it easy to match start and stop records in a log file. Acct-Session ID numbers restart at 1 each time the router is power-cycled or the software is reloaded.

Class (attribute 25) --An accounting attribute. Arbitrary value that the network access server includes in all accounting packets for this user if the attribute is supplied by the RADIUS server.

L2F --Layer 2 Forwarding. A Layer 2 tunneling protocol that enables an ISP or other access service to create a virtual tunnel to link customer remote sites or remote users with corporate home networks. In particular, a network access server (NAS) at the ISP point of presence (POP) exchanges PPP messages with the remote users and communicates by L2F or L2TP requests and responses with the customer tunnel server to set up tunnels.

NAS --network access server. A Cisco platform (or collection of platforms, such as an AccessPath system) that interfaces between the packet world (for example, the Internet) and the circuit world (for example, the public switched telephone network).

NAS-IP Address (attribute 4) --Specifies the IP address of the network access server that is requesting authentication. The default value is 0.0.0.0/0.

PPP --Point-to-Point Protocol. Successor to SLIP that provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. Whereas SLIP was designed to work with IP, PPP was designed to work with several network layer protocols, such as IP, IPX, and ARA. PPP also has built-in security mechanisms, such as CHAP and PAP. PPP relies on two protocols: LCP and NCP.

RADIUS --Remote Authentication Dial-In User Service. RADIUS is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

VPN --A system that permits dial-in networks to exist remotely to home networks, while giving the appearance of being directly connected. VPNs use L2TP and L2F to terminate the Layer 2 and higher parts of the network connection at the LNS instead of the LAC.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.